

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
ON APPEAL FROM THE EXAMINER TO THE BOARD
OF PATENT APPEALS AND INTERFERENCES**

In re Application of: Paul Gassoway
Serial No.: 10/849,318
Filing Date: May 19, 2004
Group Art Unit: 2436
Confirmation No.: 5789
Examiner: Oscar A. Louie
Title: *Method and System for Computer Security*

MAIL STOP APPEAL BRIEF - PATENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

REPLY BRIEF

Pursuant to 37 C.F.R. § 1.193, Appellants respectfully file this Reply Brief in response to the Examiner's Answer dated January 27, 2011.

ARGUMENTS

Appellants filed an Appeal Brief on November 15, 2010, explaining clearly and in detail why the rejections of the claims in the final *Office Action* are improper. While Appellants appreciate the Examiner's thoughtful consideration of this case and the Examiner's response in the Examiner's Answer dated January 27, 2011, Appellants respectfully submit that these rejections continue to be improper and should be reversed by the Board. . Appellants' address the Examiner's responses below.

I. Claims 1-2, 4, 7-8, 10, 13-14, 16, 19-20, and 22 are allowable over the Vaidya-Coleman combination.

In the Appeal Brief, Appellants sought to demonstrate that *Vaidya-Coleman* does not disclose, teach, or suggest each and every element recited in Appellants' Claims 1-2, 4, 7-8, 10, 13-14, 16, 19-20, and 22. For example, with regard to independent Claim 1, Appellants demonstrated that the proposed *Vaidya-Coleman* does not disclose, teach, or suggest at least the following claim elements:

*determining an initial system certainty value for the computer system;
increasing the system certainty value if the received data does not
match a signature in the database;
decreasing the system certainty value if the received data matches a
signature in the database; and*

First, Appellants argued that *Coleman*, which is cited by the Examiner as disclosing each of the above recited claim elements, does not disclose "an initial system certainty value." Rather, *Coleman* discloses "maintain[ing] a running mistrust level for each wireless network device 36, 38 and [wireless access point (WiAP)] 16, 16' in the [Wireless Network (WiNet)] 18 based on WiNet 18 traffic/event data 100 received at [Cooperative Decision Engine (CDE)] 76." (*Coleman*, paragraph 102). Thus, the mistrust levels disclosed in *Coleman* correspond to individual levels associated with each wireless network device and access point located within a computer system. There is no disclosure, teaching, or suggestion of an initial system certainty value for the computer system. Furthermore, since the "mistrust level" of *Coleman* measures the amount of mistrust and is increased as the mistrust increases (*Coleman*, Table 1, page 7), the "mistrust level" of *Coleman* is actually opposite to Appellants' claimed "system certainty value." Accordingly, *Coleman* and the proposed

Vaidya-Coleman combination, as relied upon by the *Final Office Action*, does not disclose, teach, or suggest “determining an initial system certainty value for the computer system,” as recited in Claim 1.

In response, the Examiner states that “appellant’s claim language does not clearly claim that the entire computer system itself performs the determination of the initial system certainty value fro the computer system itself based on the detection of intrusions in the incoming data packets.” (*Examiner’s Answer*, page 15). However, Appellants’ claim does, in fact, recite a method for “maintaining security of a computer system” wherein that computer system comprises a memory and a central processing unit and wherein the method includes “determining an initial system certainty value for the computer system.” Appellants respectfully submit that because *Coleman* discloses a feedback engine that maintains a mistrust level for each wireless device and network accesses point, *Coleman* does not disclose, teach, or suggest “determining an initial system certainty value for the computer system,” as recited in Claim 1.

Second, Appellants argued that even if one considers the mistrust levels disclosed in *Coleman* to correspond to Appellants’ “initial system certainty value” (a point Appellant does not concede and disputes above), *Coleman* fails to disclose, teach, or suggest the steps of “increasing the system certainty value if the received data does not match a signature in the database” and “decreasing the system certainty value if the received data matches a signature in the database,” as recited in Appellant’s Claim 1. Specifically, Appellants showed that cited portions of *Coleman* merely disclose adjusting the mistrust levels based on timing, manual intervention, or re-authentication. (*Coleman*, paragraph 0121). For example, *Coleman* discloses:

A decrement timer D1 is maintained on the RIAFE 86 for each WiAP 16 or wireless network device 36,38 . . . whose mistrust level exceeds zero. The decrement timer is reset whenever an anomalous event occurs at the given wireless network device, or when the operational protection suite is cycled. The mistrust level is decremented in the following way: if the decrement timer exceeds the mistrust level decrement interval from the operational protection suite, or if mistrust level four has been reached and the wireless network device 36, 38 successfully re-authenticates and there is successful login on the wireless device, then the mistrust level for that device is decremented by one.

At any time, the network administrator 92 may manually reset the mistrust level for a given wireless network device 36, 38 or WiAP 16 to any value.

Through these specific mechanisms, the mistrust levels are selectively decremented by the RIAFE 86 and wireless network devices 34, 36 or WiAP 16 can return to a stable, innocuous condition if anomalous events cease to occur.

(*Coleman*, paragraphs 123-124). Thus, *Coleman* merely discloses decrementing the mistrust level if a predetermined amount of time passes and no anomalous event is detected, if the device is reauthenticated, or if the network administrator intervenes. This is not analogous to “increasing the system certainty value if the received data does not match a signature in the database” and “decreasing the system certainty value if the received data matches a signature in the database,” as recited in Appellant’s Claim 1.

In response, the Examiner states that “*Coleman* et al. do[es] teach a “mistrust level” which is adjusted by increasing/decreasing the value based on detection of an anomaly . . .” (*Examiner’s Answer*, page 17). However, as discussed above, *Coleman* disclose that “RIAFE 86 maintains a running mistrust level for each wireless network device 36, 38 and each WiAP 16, 16’.” (*Coleman*, paragraph 100). Though *Coleman* discloses that the mistrust level of each device is “initialized to zero, then incremented or decremented by the RIAFE 86,” *Coleman* actually discloses that the mistrust level is increased in response to detecting an anomaly. (*Coleman*, paragraph 103; Table 1). Thus, the mistrust level is increased an appropriate amount “based on the type of anomaly detected” because “different attacks are assigned different weights.” (*Coleman*, paragraph 102). Accordingly, when a digital signature mismatch is detected, the mistrust level would be increased an appropriate number of levels based on the weight assigned to a signature mismatch. (*Coleman*, paragraph 102-104; Table 1). This is directly opposite to Appellants’ steps of “increasing the system certainty value if the received data does not match a signature in the database” and “decreasing the system certainty value if the received data matches a signature in the database,” as recited in Appellant’s Claim 1.

For at least these reasons, Appellants continue to respectfully submit that the rejection of Claim 1 is improper and request that the rejection be withdrawn. For analogous reasons, Appellants also submit that the rejections of independent Claims 7, 13, and 19 are improper and request that these rejections also be withdrawn.

II. Claims 3, 9, 15, and 21

In the Appeal Brief, Appellants sought to demonstrate that *Vaidya-Coleman* combination does not disclose, teach, or suggest each and every element recited in Appellants' Claims 3, 9, 15, and 21. First, Appellants argued that *Coleman*, which is cited by the Examiner as disclosing each of the above recited claim elements, does not disclose a "system certainty value." This continues to be Appellants position. Appellants refer the Board to Appellants' arguments above with respect to Claim 1 and submit that the arguments are equally applicable to Claim 3, which depends from Claim 1.

Second, Appellants argued that *Coleman* does not disclose that "the increased or decreased certainty value becomes the initial system value." As previously discussed by Appellants, *Coleman* provides an Equation 9 for calculating the new mistrust level, which takes into account the old mistrust level, a weighted anomaly, and a mistrust level decrement value. (*Coleman*, paragraph 118). Thus, the new mistrust level is calculated using a predetermined calculation having multiple variables and that one of these variables is the old mistrust level. There is no disclosure that "the increased or decreased certainty value becomes the initial system value," as recited in Claim 3.

In response, the Examiner states that "by definition, the current mistrust level after each increment/decrement would be the new 'initial system certainty value'; that is, when the next determination is made to further increment/decrement the mistrust level, the newly adjusted mistrust level is the new 'initial system certainty value.'" (*Examiner's Answer*, pages 19-20). Appellants respectfully disagree. There is no such disclosure in *Coleman*. Rather, *Coleman* discloses that "[t]he mistrust level of network devices 34, 36 and WiAPs 16, 16' is initialized to zero, then incremented or decremented by the RIAFE 86." (*Coleman*, page 103). The mistrust level is then incremented or decremented "[b]ased on the confidence metric and the type of anomaly detected." The mistrust level is then reset to zero when a predefined period of time passes without an anomaly, a mistrust level of four has been reached and the device is re-authenticated, or when a network administrator manually intervenes. (*Coleman*, paragraph 121). *Coleman* and thus, the proposed combination, does not disclose, teach, or suggest that "the increased or decreased certainty value becomes the initial system value," as recited in Claim 3.

For at least these reasons, Appellant respectfully submits that the rejection of dependent Claim 3 is improper and request that the rejection be withdrawn. For analogous

reasons, Appellant also submits that the rejections of dependent Claims 9, 15, and 21 are improper and should also be withdrawn.

III. Claims 5, 11, 17, and 23 are allowable over the Vaidya-Coleman-Nakae combination.

Claims 5, 11, 17, and 23 depend from Claims 1, 7, 13, and 19, respectively. As shown above, Appellant respectfully contends that the proposed *Vaidya-Coleman* combination fails to disclose, teach, or suggest every limitation of these independent base claims. As such, Appellant respectfully contends that Claims 5, 11, 17, and 23 are allowable over the cited references at least as a result of their respective dependencies upon allowable independent Claims 1, 7, 13, and 19. Accordingly, Appellant requests reconsideration and allowance of Claims 5, 11, 17, and 23.

IV. Claims 6, 12, 18, and 24 are allowable over the Vaidya-Coleman-Nakae-Moran combination.

In the Appeal Brief, Appellants sought to demonstrate that *Vaidya-Coleman-Nakae-Moran* does not disclose, teach, or suggest each and every element recited in Appellants' Claims 6, 12, 18, and 24. Specifically, Appellants argued that the cited references do not disclose that the step of forwarding further comprises "generating a message log to indicate that data matching a signature was forwarded." Rather *Moran*, which is relied upon by the Examiner for disclosure of the recited claim elements, merely discloses "a mechanism for checking timestamps, configured to identify backward and forward time steps in a log file." (*Moran*, Column 4, lines 28-31). While this discloses identifying time steps in a log file, *Moran* fails to disclose, teach, or suggest actually generating a log file, much less a log file that indicates that data matching a signature was forwarded. Accordingly, *Moran* and the proposed *Vaidya-Coleman-Nakae-Moran* combination fails to disclose, teach, or suggest "wherein the step of forwarding further comprises generating a message log to indicate that data matching a signature was forwarded," as recited in Claim 6.

In response, the Examiner points to various portions of *Moran* that mention a "log." For example, the Examiner points to Column 10, lines 50-53 for further disclosure of the claim elements. (*Examiner's Answer*, page 21). However, the cited portion merely discloses

that “some tools allow a system administrator to be alerted whenever an entry matching any of the patterns he has specified is written to a designated log file.” (*Moran*, Column 10, lines 50-53). Thus, the system administrator is notified in response to an entry being written to a log file. Thus, the log merely includes matching patterns. The log of *Moran* is not a **message log that indicates that data has been forwarded**. Further, notifying the system administrator in response to a matching pattern being written to a log file is in direct contrast to Applicants’ claim language that recites “generating a message log to indicate that data matching a signature was forwarded,” as recited in Claim 6.

As another example, the Examiner points to Column 4, lines 28-31. (*Examiner’s Answer*, page 21). However, the cited portion merely discloses that the “intrusion detection system comprises a mechanism for checking timestamps, configured to identify backward and forward time steps in a log file, correlate them with other events, and assign a suspicion value to a record associated with an event.” (*Moran*, Column 4, lines 28-33). Again, the cited portion does not at all relate to a **message log**. Furthermore, disclosing a mechanism for checking timestamps and correlating the timestamps with other events is not analogous to “generating a message log to indicate that data matching a signature was forwarded,” as recited in Claim 6.

The Examiner also points to Column 11, lines 41-44. (*Examiner’s Answer*, page 21). However, the cited portion merely discloses that “[s]ome of the programs most likely to be involved in an attack produce log entries for significant events.” (*Moran*, Column 11, lines 41-42). Thus, this part of the disclosure relates to the program that is actually producing the attack. Stated differently, during an attack, the program producing the attack may produce log entries for significant events. According to *Moran*, some of these attacking programs “put related, often overlapping, information into different log files.” (*Moran*, Column 11, lines 42-44). *Moran* makes clear that these are “commonly available hacker tools that help an attacker hide his tracks by deleting selected entries from these files.” (*Moran*, Column 11, lines 42-44). Again, the cited portion does not at all relate to a message log. Certainly, it does not disclose, teach, or suggest “generating a message log to indicate that data matching a signature was forwarded,” as recited in Claim 6.

Additionally, the Examiner points to Column 20, lines 1-3 and 27-35. However, the cited portions relate to “login correlations.” Specifically, *Moran* discloses that in a UNIX embodiment, the init “creates a getty process for all lines on which logins are to be enabled.”

(*Moran*, Column 19, lines 49-51). “If the user successfully logs in, the login process exec’s the specified shell for the user (exec replaces the program running as the current process with a new program . . .).” (*Moran*, Column 19, lines 55-59). In contrast, “[a] failed login attempt or the end of a successful login session generates a signal to the getty that triggers it to re-initialize the line and await the next login attempt.” (*Moran*, Column 19, lines 59-62). According to *Moran*, “when a valid username-password pair is entered,” UNIX typically “writes a record to the utmp and wrmp files and updates the last log file.” (*Moran*, Column 19, line 66 through Column 20, line 3). Thus, *Moran* merely discloses writing in a login log when a user successfully logs into the system. Again, the cited portion does not at all relate to a message log. Certainly, it does not disclose, teach, or suggest “generating a message log to indicate that data matching a signature was forwarded,” as recited in Claim 6.

For at least these reasons, Appellant respectfully submits that the rejection of dependent Claim 6 is improper and request that the rejection be withdrawn. For analogous reasons, Appellant also submits that the rejections of dependent Claims 12, 18, and 24 are improper and should also be withdrawn.

ATTORNEY DOCKET NUMBER:
063170.7177

PATENT APPLICATION
USSN 10/849,318

9

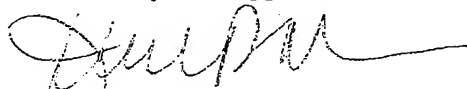
CONCLUSION

Appellants have demonstrated that the present invention, as claimed, is clearly distinguishable over the prior art cited by the Examiner. Therefore, Appellants respectfully request the Board to reverse the final rejections and instruct the Examiner to issue a Notice of Allowance with respect to all pending claims.

No fees are believed due; however, the Commissioner is authorized to charge any additional fees or credits to Deposit Account No. 02-0384 of Baker Botts, L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Appellants



Jerini R. Moen
Reg. No. 52,038
(214) 415-4820

Dated: March 16, 2011

Correspondence Address:

at Customer No. **05073**